

D-23

1 Jack Russo (Cal. Bar No. 96068)  
2 Christopher Sargent (Cal. Bar No. 246285)  
3 COMPUTERLAW GROUP LLP  
4 401 Florence Street  
5 Palo Alto, CA 94301  
6 (650) 327-9800 office  
7 (650) 618-1863 fax  
8 jrusso@computerlaw.com  
9 csargent@computerlaw.com

10 Attorneys for Third Parties  
11 THEODORE KRAMER and  
12 THOMAS SCARAMELLINO

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
SUPERIOR COURT OF CALIFORNIA  
COUNTY OF SAN MATEO

**Six4Three**, a Delaware limited liability  
company,

Plaintiff;

v.

**Facebook, Inc.**, a Delaware corporation;  
**Mark Zuckerberg**, an individual;  
**Christopher Cox**, an individual; **Javier**  
**Olivan**, an individual; **Samuel Lessin**, an  
individual; **Michael Vernal**, an individual;  
**Ilya Sukhar**, an individual; and **Does 1-50**,  
inclusive,

Defendants.

**FILED**  
**SAN MATEO COUNTY**

APR 15 2019

Clerk of the Superior Court

PA

CLERK

Case No. CIV533328

Assigned for all purposes to Hon. V.  
Raymond Swope, Dep't 23

**DECLARATION OF JACK RUSSO IN SUPPORT  
OF OPPOSITION TO DEFENDANT FACEBOOK,  
INC.'S SECOND IMPROPER MOTION FOR  
RECONSIDERATION TO OPEN DISCOVERY**

CIV533328

DIO

Declaration in Opposition  
1766212



**RECEIVED**

APR 15 2019

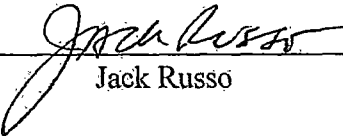
SUPERIOR COURT  
CNL DIVISION

1 I, Jack Russo, declare under penalty of perjury as follows:

2 1. My name is Jack Russo. I am managing partner of Computerlaw Group LLP and  
3 counsel for third parties Theodore Kramer and Thomas Scaramellino. I am a member in good  
4 standing of the California State Bar and have been since I was admitted over thirty-five (35)  
5 years ago. I make the following statements based on my personal knowledge, and I believe them  
6 to be true. I could and would testify competently if called as a witness.

7 2. On April 12, 2019 I sent a letter to Joshua Lerner, Counsel for Defendant  
8 Facebook. A true and correct copy of this letter is attached as **Exhibit 1**.

9  
10 I declare under penalty of perjury under the laws of the State of California that the  
11 foregoing is true and correct and that this declaration was entered into on April 12, 2019 in Palo  
12 Alto, California.

13   
14 Jack Russo

# **EXHIBIT 1**

# COMPUTERLAW GROUP LLP

ATTORNEYS AT LAW  
401 FLORENCE STREET

PALO ALTO, CALIFORNIA 94301  
COMPUTERLAW.COM

TELEPHONE  
(650) 327-9800

FAX  
(650) 618-1863

April 12, 2019

## Via Email

Joshua Lerner, Esq.  
Durie Tangri LLP  
217 Leidesdorff Street  
San Francisco, CA 94111  
jlerner@durietangri.com

Re: Six4Three, LLC v. Facebook, Inc. et al.  
San Mateo Super. Ct. Case No. CIV 533328

Dear Mr. Lerner:

Do you not see the irony in Facebook now claiming how “obvious” it is that Mr. Kramer, a layperson, was supposed to treat the U.K. Parliamentary Orders as though they could be readily ignored, while at the same time Facebook was given repeated notice but failed to take any legal steps against MP Collins or his DCMS Committee? Think about it. Perhaps 20-20 “hindsight” is perfect, but Facebook could not sit on its hands nor refuse to fully disclose to the Court the actual electronic exchanges and other correspondence which it has had with Mr. Collins and/or his Committee and/or others in Parliament about any of this. The entire rationale of Section 16 of the Protective Order puts squarely on Facebook the obligation to take steps following notice, and there is no dispute that multiple notices were given to Facebook before any disclosure took place. This is especially so because Facebook knows that neither Mr. Kramer nor 643 has the ability or financial resources to do so. As to the rest of your letter, we believe Mr. Kramer acted appropriately and in good faith in the face of a real threat to his freedom in London following service of the contempt notices on him because:

1. It is a well-established that the power to punish contempt is not restricted to the Judiciary, and that administrative bodies such as the Senate have the power to punish contempt for their orders by direct imprisonment, criminal charges, or otherwise. Barenblatt v. U.S., 360 U.S. 109, (1959); *see also* In re Battelle, 207 Cal. 227, (1929). Given the many administrative investigations and/or proceedings currently pending against Facebook,<sup>1</sup> it is surprising that you appear to be arguing that Section 16 of the Stipulated Protective Order applies only to “a subpoena or a court order issued in other litigation.” If the Senate subpoenaed Facebook for these same documents, would Section 16 not apply in that circumstance either? Think about it.

2. Neither your letter nor your November 28, 2018 filings with the Court address whether Facebook has taken any steps to mitigate the effects of the DCMS Committee’s seizure of Facebook’s allegedly confidential information. Your letter contains a link describing public communications between Mr. Richard Allen and Mr. Collins *following* the disclosure but does not provide any further information regarding any attempts to carry out your obligation under Section 16 of the Stipulated Protective Order to “promptly notify in writing the party who caused

---

<sup>1</sup> Facebook, Inc. is currently the subject of inquiries, investigations, or other legal entanglements with the Federal Trade Commission, The Federal Bureau of Investigation, The Department of Justice, The Department of Housing and Urban Development, The U.S. Senate Commerce Committee, the U.S. Senate Select Committee on Intelligence, The U.S. House of Representatives Committee on Energy and Commerce, The European Commissioner for Justice and Consumers, The U.K.’s Information Commissioner, Ireland’s Data Protection Commissioner, and Australia’s Information Commissioner. This list is nowhere near exhaustive.

Joshua Lerner  
April 12, 2019  
Page 2

the subpoena or order to issue in the other litigation that some or all of the material covered by the subpoena or order is subject to this Stipulated Protective Order.” Did you or your office or anyone else for Facebook (including any lawyers it employs in London) take any such mitigating steps? Specifically:

- Have you provided to the Court and the parties any such exchanges between yourselves and Mr. Collins and his Committee as counsel for Plaintiff has done?
- Has your office provided the parties or the Court with any notices sent to Twitter or other online services about the propagation of Facebook’s alleged confidential information on their platforms?
- Has your office taken any steps, regardless of Section 16 of the Protective Order, to limit the disclosure of Facebook’s alleged confidential information?
- If the information is truly “trade secret” and if MP Collins did not act in accord with applicable law then his actions must, in your view, violate Facebook intellectual property rights; isn’t failure to enforce those rights a knowing waiver of them?

Direct answers to these questions are needed by the Stipulated Protective Order and attempts to avoid these issues through rhetoric will certainly not be well taken by us or the Court.

3. Notwithstanding your denial of Ms. Mehta’s statement at the March 15 Hearing that Facebook communicated with Parliament, your alternate theory, that “Facebook communicated with the DCMS Committee following Mr. Kramer’s improper disclosure but before the DCMS Committee publicized the documents” raises more questions than it answers. As both the news article included in your letter and the Declaration of Laura E. Miller of November 28, 2018 demonstrate, Facebook has substantial legal resources in the U.K. and in areas of U.K. law, including having a Member of the House of Lords (the Hon. Richard Allen) on its payroll. Given these resources, why is it that Facebook waited until *after* Mr. Kramer disclosed the documents to communicate with the DCMS Committee? Are you contending that in the critical 72-hour timeframe between notification by Mr. Godkin and the actual disclosure, your office wrote to the Court to stress that there was an “imminent violation of the protective order,” but it did not have the time or will to take action to cooperate with counsel for Six4Three and prevent the disclosure from actually occurring, as it very likely could have? An email summarizing Mr. Gordon’s conclusions to counsel for Six4Three would have been a very low-cost option to your client and would have likely prevented the ensuing mess. Instead, in your sequence of events, your office exercised none of its options to avert the impending tangle.

4. Your letter does not address the multiple factual inaccuracies made by you and your office to the Court summarized in Exhibit F of my previous letter and attached hereto for your convenience. We can only assume that you have had time to review this evidence thoroughly and discuss it with your client. It remains imperative that you take immediate steps to correct these false representations, and it is unfortunate that you have not elected to do so already. Our clients will and do otherwise reserve all of their rights and remedies.

Joshua Lerner

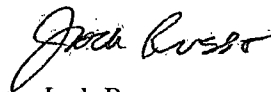
April 12, 2019

Page 3

5. Finally, pursuant to your invitation, I have reviewed your firm's submissions to the Court dated November 28, 2018 once again. I note that the Brief re: Court's Order Dated November 20, 2018 insists that an Order to Show Cause be issued, and that Contempt Proceedings occur "promptly." It is now nearly four months later, and Facebook has taken no steps on it alleged continues to drag its feet on a Request for an Order to Show Cause. Why?

Facebook can garner far more through cooperation with Mr. Kramer than with continuing threats against him. I suggested this last December when I first appeared in this case on his behalf. I am suggesting it again. It seems to me that it would be far more helpful for our firms to cooperate on behalf of our respective clients than to continue contesting the fact that Mr. Collins and his Committee used Parliamentary process against both of our clients. Let me know if you and your client are open to a more productive dialogue.

Very truly yours,


A handwritten signature in cursive script, appearing to read "Jack Russo".

Jack Russo

cc: Counsel of Record via Email

Enclosure


"Offending" Summary Compared to Superior Court Public Docket


<b>"Offending" Summary</b>	<b>Superior Court Public Docket</b>
	<p data-bbox="833 342 1412 1223">"643's review of Facebook's initial production also clearly reveals the identities of the decision-makers and rough timeframes under which the decision at the heart of 643's [Second Amended Complaint] was made.... It is abundantly clear from Facebook's production that the deceptive, anti-competitive and fraudulent scheme alleged by 643 in its SAC was spearheaded by Mark Zuckerberg (CEO) sometime prior to October 2012 and involved at least the following individuals: Sam Lessin (VP Product Management), Chris Cox (Chief Product Officer), Javier Oliván (VP Growth), Michael Vernal (VP Engineering), and Ilya Sukhar (Head of Developer Products). The decision and its rationale were then communicated to the next layer of management, including Douglas Purdy (Director of Engineering), Constantin Koumouzelis (Product Manager), Dan Rose (VP Partnerships and Platform Marketing), Ime Archibong (Director, Strategic Partnerships, Monica Bickert (Head of Global Policy Management), Justin Osofsky (Director, Platform Operations) and others, from late 2012 through the middle of 2013." Discovery Proposal Pursuant to Court's December 13, 2016 Order, filed January 20, 2017, at 6-7.</p> <p data-bbox="833 1255 1412 1744">"Plaintiff's review of Facebook's files confirms this suspicion and reveals abundant evidence specifically describing the negotiation of multiple, tied contracts (at least one contract to extract advertising payments and another to provide special data access). Facebook's files further confirm that significant engineering effort and capital was deployed in executing these contracts. As such, Facebook and its partners are separate entities undertaking acts in concert which caused proximate harm to Plaintiff, other companies, and the public by actually depriving the marketplace of competition." Reply to Opposition to Motion to Remand, filed February 9, 2017, at 9-10 (3:17-cv-00359-WHA, N.D. Cal.)</p> <p data-bbox="833 1776 1412 1902">"The evidence submitted by Plaintiff supporting these claims consists of a large volume of internal discussions among Facebook employees regarding Defendants' motivations for, and</p>





	<p>implementation of, various decisions related to access to Facebook's software APIs, primarily from 2012 to 2015, as well as reliance by Plaintiff on false representations concerning such access and damages suffered by Plaintiff when the promised access was eliminated, including interference in its contractual and prospective relations with customers." Proposed Order Denying Individual Defendants' Special Motion to Strike, filed July 9, 2018, at 11.</p> <p>"In mid-to-late 2012, the Conspiring Facebook Executives began communicating to various Facebook employees that data access would be severely restricted to many companies that built applications related to contacts and calendar management, messaging, photo sharing, video sharing and streaming, online dating, lifestyle, games, news, books, fitness and various utility applications." Fifth Amended Complaint, filed January 12, 2018 (5AC) ¶ 89 (39:14-18); Fourth Amended Complaint, filed November 1, 2017 (4AC) ¶ 83 (30:24-28)</p> <p>"Facebook architected its Platform in a manner designed to violate user privacy as early as 2009, which entailed: (1) separating the privacy settings for data a user shared with friends in apps the user downloaded ("user data") with the privacy settings ("Apps Others Use" settings) for data the user shared with friends in apps the friends downloaded ("friend data") (Jud. Not. Dec., ¶ 32, <u>Ex. 31</u>, Federal Trade Commission Complaint, at 4-7); (2) hiding the Apps Others Use settings to ensure most Facebook users were not aware that these settings were distinct from the main privacy settings (<i>Id.</i>, at 4-9); (3) making the default setting for sharing data with Apps Others Use set to "on" so Facebook could funnel more data to developers under the guise of user consent (<i>Id.</i>, at 7-11); and (4) deliberately failing to pass privacy settings for data transmitted to developers via Facebook's APIs, signaling to developers that all friend data was public and could be treated as such." Opposition to Individual Defendants' Anti-SLAPP Motion, filed May 17, 2018, at 2-3.</p>
	<p>"Zuckerberg then brought Vernal directly into the discussions in late 2012 in order to oversee and implement the bait and switch plan. Upon</p>


	<p>information and belief, Vernal planned a public announcement of this decision at the end of 2012 but Zuckerberg prohibited the announcement.” 5AC ¶ 85 (37:14-17).</p> <p>“Upon information and belief, starting in mid-to-late 2012 and continuing through mid-2013, Zuckerberg communicated the decision he had already made to restrict Graph API data in order to restrain competition for Facebook’s new products and to prop up Facebook’s new mobile advertising business to senior executives on the Platform team, including Vernal (VP Engineering for Platform), Sukhar (Head of Developer Products), Doug Purdy (Director of Engineering for Platform), Eddie O’Neil (Product Manager for Platform), and other senior members of the Platform and developer teams. Upon information and belief, starting in late 2012 and throughout 2013, at Zuckerberg’s instruction, Vernal, Sukhar, Purdy, O’Neil and others began implementing Zuckerberg’s decision to restrict data access for anti-competitive reasons under the Reciprocity Policy framework. Upon information and belief, the Platform team, managed by Vernal, was working on a public announcement of these changes to be released before the end of 2012. However, the changes were not publicly disclosed.” 5AC ¶ 214 (76:1-12); 4AC ¶ 208 (66:10-21).</p> <p>“The Conspiring Facebook Executives made various layers of management aware of this decision on a need-to-know basis periodically from late 2012 until late 2013 and, at all times, required such employees to actively conceal and/or make only partial disclosures of these material facts.” 4AC ¶ 106 (40:24-27).</p> <p>“The Platform team, managed by Vernal, was working on a public announcement of these changes to be released before the end of 2012. However, Zuckerberg directed Vernal not to disclose these changes but to instead extract payments from Developers upon threat of being shut down from the public Platform APIs. In other words, Zuckerberg directed Vernal to privately and secretly enforce these changes while continuing to mislead the general public and Developers, including Styleform.” Styleform</p>
--	--

	<p>Complaint, filed November 2, 2018 (SC) ¶ 17 (7:13-18).</p> <p>“Instead, Facebook noted in its public announcement only that some ‘rarely used’ APIs would be shut down. This statement was false, and Defendants knew it to be false at the time they made it. In fact, the endpoints shut down on April 30, 2015 (the very same ones Zuckerberg secretly restricted in October and November 2012) were the most widely used APIs in Facebook Platform.” SC ¶ 163 (64:3-7).</p>
	<p>“In the summer and fall of 2012, Lessin worked with Zuckerberg and other Facebook executives like Sheryl Sandberg, Andrew Bosworth and Dan Rose to weaponize developers’ reliance on Facebook Platform by threatening to break many software applications unless the developer made significant purchases in unrelated advertising using Facebook’s new mobile advertising product. Upon information and belief, Lessin was instrumental in developing the plan whereby Facebook approached companies to buy advertising under the threat that if they did not do so, Facebook would break their applications by removing access to public Platform data.” SAC ¶ 26 (13:18-25).</p> <p>“This reference to Facebook as a ‘monopolist’ and as ‘monopolizing for itself’ is not sufficient to make any reasonable determination as to whether Facebook’s conduct was unilateral or in concert with other partners with which it executed binding agreements to extract large advertising payments in exchange for their continued access to data that had been shut off to all other companies, thereby giving these partners an insurmountable competitive advantage in various software markets.” Reply to Opposition to Motion to Remand, filed February 9, 2017, at 2 (3:17-cv-00359-WHA, N.D. Cal.)</p> <p>“Further, Zuckerberg’s bait and switch scheme violates the Cartwright Act as Facebook maliciously tied its Platform APIs (the tying product) to its Neko advertising product (the tied product), which are entirely unrelated and distinct products. Facebook refused to offer the Platform APIs unless companies purchased Neko advertising. Facebook had sufficient economic</p>

	<p>power in the market for Platform APIs (it was the sole provider of these APIs) to coerce companies into purchasing Neko advertising, and the tying arrangement prohibited an estimated 40,000 companies from purchasing advertising (the tied product) as they no longer had products to advertise. CACI (2017) (Bus. &amp; Prof. Code, § 16727)...” Opposition to Individual Defendants’ Anti-SLAPP Motion, filed May 17, 2018, at 13-14, fn. 25.</p>
	<p>“Upon information and belief, Facebook at no time provided access to the Graph API on an equal basis, but rather offered large companies unfair competitive advantages and special access to data in exchange for unrelated advertising purchases or other in-kind consideration at the expense of small or new companies attempting to compete in Facebook’s operating system.” 5AC ¶ 2 (3:5-8); 4AC ¶ 2 (3:4-7).</p> <p>“Upon information and belief, many Developers with close relationships to Facebook and who paid substantial sums of cash or other financial consideration continue to access this data in some form, notwithstanding that it has been restricted to all other software companies.” 5AC ¶ 101 (45:3-6).</p> <p>“Upon information and belief, working in concert with other Facebook executives and employees and other large companies that were close partners, Zuckerberg implemented a plan to deny access to many applications on Facebook Platform on the primary or exclusive basis that these applications were competitive with current or future products offered by Facebook or Facebook’s close partners. Upon information and belief, Defendants’ anti-competitive conduct was undertaken in concert with other large companies to oligopolize various software markets that Defendants continued to represent would operate on fair and equal terms.” 4AC ¶ 4 (3:24-4:4).</p> <p>“Tinder, along with a number of other companies that rely upon photo or friend information from Facebook and executed whitelist agreements under Facebook’s ‘reciprocity principle,’ are competitors of Plaintiff. It is entirely plausible that Facebook and each of these entities constitute</p>

	<p>a trust under the Cartwright Act as they engaged in 'a combination of capital, skill, or acts by two or more persons to achieve an anticompetitive end.' The anticompetitive ends encompass restrictions in trade or commerce, the reduced production of a commodity and contracts to preclude free competition, and the combination of interests in connection with a sale of advertising. For instance, the number and kinds of software applications from which consumers could choose decreased precipitously once Facebook shut down access to its data. Consumers were forced to choose from a much smaller pool of applications – those developed exclusively by Facebook or companies from which Facebook could extract large advertising payments.” Reply to Opposition to Motion to Remand, filed February 9, 2017, at 14 (3:17-cv-00359-WHA, N.D. Cal.)</p>
	<p>“At Zuckerberg’s personal direction, Facebook used its platform as a weapon to gain leverage against competitors in a host of ways, threatening to shut down access to publicly available data to any company that crossed Facebook’s radar in a wide range of circumstances, including threats to shut down data access; unless the company sold to Facebook for a purchase price below their fair market value; unless the company purchased large amounts of unrelated advertising with Facebook; unless the company transferred intellectual property to Facebook; or unless the company fed all of its data back to Facebook, where it would then be available to the company’s competitors, placing the company’s business at great risk.” 5AC ¶ 3 (3:9-17). 4AC ¶ 3 (3:8-16).</p> <p>“Beginning in 2012 and continuing until 2015, at Zuckerberg’s personal direction, Facebook executives instructed their subordinates to identify categories of applications that would be considered competitive and to develop a plan to remove access to critical data necessary for those applications to function, thereby eliminating competition across entire categories of software applications....” 5AC ¶ 7 (5:3-7); 4AC ¶ 7 (4:27-5:3).</p> <p>“Zuckerberg held discussions with Defendants Cox, Olivan, and Lessin (in addition to other Facebook executives like Sheryl Sandberg, Daniel</p>

	<p>Rose, and Andrew Bosworth) where Zuckerberg communicated his decision to shut down access to Graph API data to applications that were competitive with current Facebook products and with products Facebook may choose to launch in the future, even if Facebook had not begun working on such products.” 5AC ¶ 85 (37:6-12); 4AC ¶ 79 (29:14-19).</p> <p>“Once Zuckerberg decided to remove the Graph API Data to competitors, Zuckerberg personally maintained an ever-growing list of competitors that only he could authorize blacklisting from the Graph API Data. Upon information and belief, once a Developer was blacklisted from the Graph API Data, any applications the Developer built could no longer use any of the blacklisted data that Facebook purportedly provided publicly on fair and neutral terms to all Developers. Upon information and belief, blacklisted data often included the Graph API data, including the full friends list, friends permissions and newsfeed APIs – data types that were among the most popular on Facebook Platform and upon which 643’s business and many other businesses depended.” 5AC ¶ 211 (74:7-15).</p> <p>Numerous examples of Facebook enticing companies to build their products in reliance on the Graph API, reinforcing Facebook’s false representations that Graph API is freely and equally available to all companies. 5AC ¶¶ 114-122; 4AC ¶¶ 110-117.</p>
	<p>“Decisions were made not unilaterally but in combination and concert with other large companies and exceptions were made for certain applications that are more susceptible to violating user trust or where user trust is in fact more important than in normal applications, such as applications that require payments. These exceptions demonstrate that user trust could not have been the actual reason for Facebook’s decision to restrict Graph API data.” 5AC ¶ 128 (56:18-23); 4AC ¶ 122 (47:15-20).</p> <p>“Upon information and belief, many Developers with close relationships to Facebook and who paid substantial sums of cash or other financial consideration continue to access this data in some form, notwithstanding that it has been restricted to</p>

	<p>all other software companies.” 5AC ¶ 101 (45:3-6).</p> <p>“Facebook reached an unspecified compromise with dating app Tinder that permitted some form of access to photos of mutual friends. Upon information and belief, Tinder provided highly valuable unrelated financial consideration to Facebook in exchange for this special access to data.” 5AC ¶ 66:4-7.</p> <p>“However, Facebook at no time provided access to the Graph API on an equal basis, but rather offered large Developers unfair competitive advantages and special access to data in repeated violation of user privacy and its public commitment to a level competitive playing field, in exchange for unrelated advertising purchases or other in-kind consideration at the expense of small or new Developers, like Styleform, that were attempting to compete in the Facebook Platform.” SC ¶ 5 (5:16-21)</p> <p>Referring to current Facebook policies that demonstrate Facebook still does not enforce its policies for select partners: “Only use friend data (including friends list) in the person’s experience in your app. (See <a href="https://developers.facebook.com/policy">developers.facebook.com/policy</a>, Section 3.3). This demonstrates that some Developers who have entered into special agreements with Facebook still have access to this social data notwithstanding that the data has been restricted to all other Developers. Certain large Developers with close relationships to Facebook and who paid Facebook substantial sums of cash or other financial consideration continue to have access to this data in some form, notwithstanding that it has been restricted to at least 35,000 other Developers.” SC ¶ 52 (21:27-22:6).</p> <p>Referring to more than 5,000 special agreements, which qualifies as “numerous instances”. SC ¶ 68 (26:25-26).</p>
	<p>“From 2007 through at least 2015, Facebook willfully, intentionally, recklessly, maliciously and negligently failed to pass privacy or age information when sending Developers Graph API Data. This required Developers, including 643, to incur enormous costs in order to comply with user</p>



privacy settings and age restrictions. Facebook made repeated public disclosures that withheld this fact.” 5AC ¶ 232 (84:1-5); 4AC ¶ 226 (73:16-20).

“Zuckerberg tasked Sukhar and Vernal with developing a plan to communicate and mask this fraudulent scheme to Facebook employees and, eventually, Developers and the public.” 5AC ¶ 88 (39:4-5); 4AC ¶ 82 (30:14-15).

“Further, employees were livid by the scheme when they found out in late 2013 and 2014 and many left the company. Before leaving, these employees noted that Facebook was deliberately trying to place the blame on unspecified bad actor Developers for Facebook’s own anti-competitive and privacy-violating conduct and that Facebook was succeeding in doing so.” SC ¶ 26 (10:16-19).

“Contrary to its public representations, when Facebook restricted the Graph API in 2015, it did not do so for the purpose of enhancing user privacy. Rather, Facebook had previously hid its privacy controls and set the default sharing setting to ‘on’ in violation of the FTC Order in order to funnel more data to Developers that agreed to Facebook’s extortion scheme that tied Platform API access to unrelated purchases in Facebook’s mobile advertising products. Facebook could have complied with the FTC Order, in 2012, by: (1) not hiding the ‘Apps Others Use’ privacy page; (2) turning the default setting to ‘off; and (3) by passing privacy information along with the data it sent through its APIs, an issue reported by Facebook employees for many years and which management willfully and deliberately decided not to fix in violation of the FTC Order. Instead, Facebook expanded the very violations at the center of the FTC’s complaint leading up to the FTC Order for the purpose of improperly oligopolizing for itself and other large Developers various attractive software markets.” SC ¶ 116 (47:7-18).


“Facebook architected its Platform in a manner designed to violate user privacy as early as 2009, which entailed: (1) separating the privacy settings for data a user shared with friends in apps the user downloaded (“user data”) with the privacy settings (“Apps Others Use” settings) for data the




user shared with friends in apps the friends downloaded (“friend data”) (Jud. Not. Dec., ¶ 32, Ex. 31, Federal Trade Commission Complaint, at 4-7); (2) hiding the Apps Others Use settings to ensure most Facebook users were not aware that these settings were distinct from the main privacy settings (*Id.*, at 4-9); (3) making the default setting for sharing data with Apps Others Use set to “on” so Facebook could funnel more data to developers under the guise of user consent (*Id.*, at 7-11); and (4) deliberately failing to pass privacy settings for data transmitted to developers via Facebook’s APIs, signaling to developers that all friend data was public and could be treated as such.” Opposition to Individual Defendants’ Anti-SLAPP Motion, filed May 17, 2018, at 2-3.

“By way of example, if User A uploaded a photo to Facebook and set the photo to ‘only me,’ only User A would be able to see the photo on Facebook.com or in the Facebook mobile app. However, because the Apps Others Use setting was hidden, not explained to users, and had the default set to ‘on’ (issues the FTC had identified in its Complaint and Order), this meant that when User B used a Developer’s app, User B would be able to see User’s A photo that was set to “only me” if User B was friends with User A. This is because Facebook did not pass the privacy settings of a data object in the most widely used Graph API endpoints, and because Facebook had ‘auto-consented’ User A to share this data in Apps Others Use without revealing this fact to User A. User B sees the photo and tells User A, and User A complains that the Developer is violating their privacy when in fact it was Facebook. The Developer could not have even known that User B was not supposed to see User A’s photo since Facebook falsely represented it handled such settings prior to sending the photo to the Developer.” SC ¶ 113 (46:5-16)

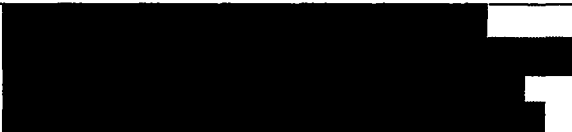
“Zuckerberg’s scheme made it impossible for Plaintiff’s business and thousands of other businesses to succeed on Facebook Platform and directly resulted in the widely reported scandal in which a developer, Cambridge Analytica, used Facebook data to influence the 2016 Presidential election....” Opposition to Individual Defendants’ Anti-SLAPP Motion, filed May 17, 2018, at 3-4.

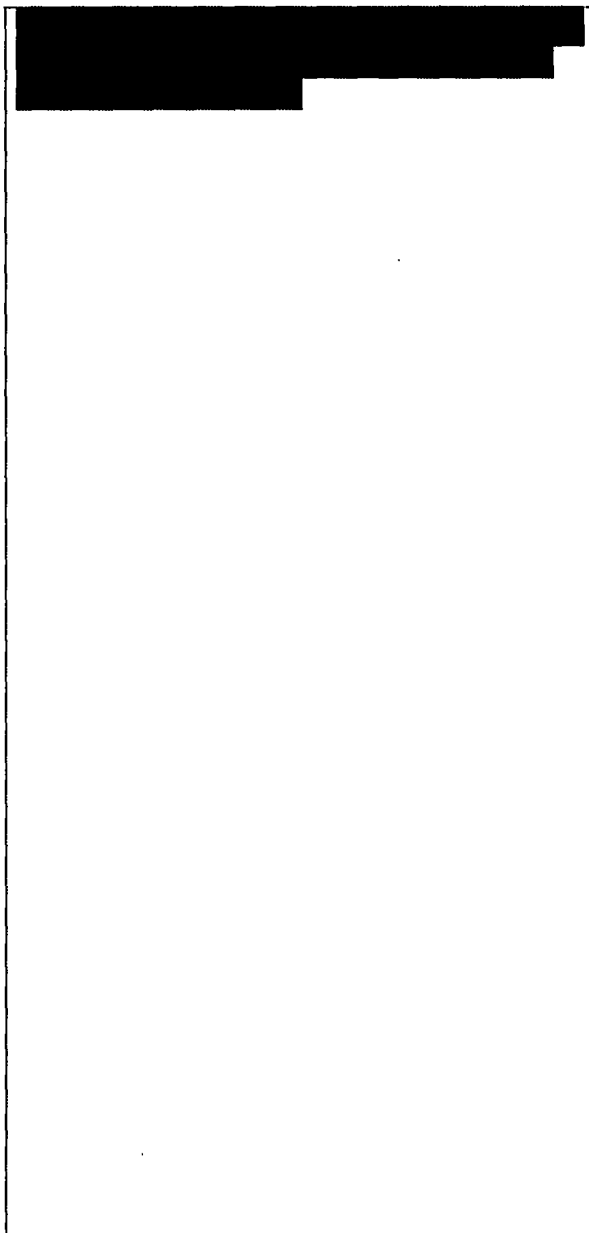

	<p>“643 could not have known that Zuckerberg had already decided to restrict access to the data necessary for 643’s technology to work, as Facebook had exclusive access to this information and had taken measures to actively conceal this fact from 643, other Developers, and the public.” 5AC ¶ 103 (45:26-46:2); 4AC ¶ 97 (37:3-6).</p> <p>“Facebook held numerous meetups, conferences, hackathons and the like in which Facebook employees trained developers like 643 to access data the conspiring Facebook Executives had already made the decision to restrict, encouraging and enticing Developers to invest time, money and resources in applications Facebook knew would not function based on decisions Zuckerberg had already made.” 5AC ¶ 114 (50:5-9); 4AC ¶ 108 (41:7-11).</p> <p>“Facebook’s public disclosure that it made these changes out of respect for user privacy is undermined by numerous Facebook projects that deliberately, willfully, intentionally, recklessly and negligently violated privacy by only making partial disclosures to Developers regarding how Facebook collected, stored, and transmitted user data. Upon information and belief, beginning at least by 2012, Olivan directed a range of projects under the supervision and direction of Zuckerberg, Cox and Lessin that deliberately, intentionally, maliciously, recklessly and negligently violated user privacy in order to effectuate Facebook’s anti-competitive scheme of baiting companies to rely on Facebook Platform.” 5AC ¶ 226 (80:25-81:6); 4AC ¶ 220 (70:25-71:5).</p> <p>Numerous examples of Facebook enticing companies to build their products in reliance on the Graph API instead of taking measures to make a full public disclosure around its treatment of user and friend data. 5AC ¶¶ 114-122; 4AC ¶¶ 110-117.</p> <p>“Zuckerberg’s scheme made it impossible for Plaintiff’s business and thousands of other businesses to succeed on Facebook Platform and directly resulted in the widely reported scandal in which a developer, Cambridge Analytica, used Facebook data to influence the 2016 Presidential election....” Opposition to Individual Defendants’ Anti-SLAPP Motion, filed May 17, 2018, at 3-4.</p>
---	---

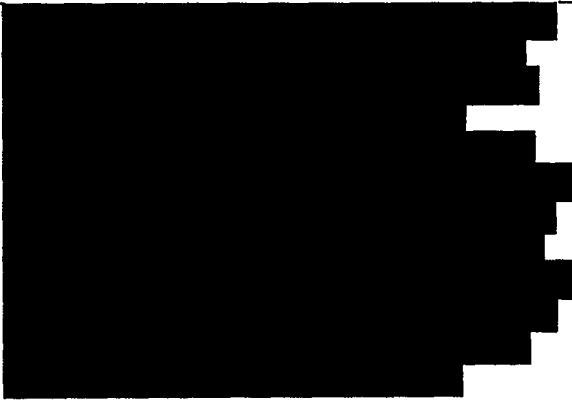
	<p>“Around the time Zuckerberg made this decision to engage in the alleged fraudulent and anti-competitive schemes, Facebook’s stock price had dropped by more than half from its initial IPO in May 2012, reaching a low of \$37 billion in September 2012. Zuckerberg personally lost approximately \$10 billion in the period during which he decided to implement the fraudulent and anti-competitive schemes.” 5AC ¶ 14 (7:20-24); 4AC ¶ 14 (7:14-18).</p> <p>“Around the time Zuckerberg made the decision to implement Facebook’s anti-competitive scheme in 2012, Facebook was experiencing substantial difficulty transitioning its service from desktop computers to mobile devices. The executive team was extremely concerned around the impact this transition would have on Facebook’s revenues, particularly in light of the fact that Facebook was planning an initial public offering (IPO) of its shares around this time.” 5AC ¶ 295 (97:19-24); 4AC ¶ 279 (84:12-17).</p> <p>“Zuckerberg’s motivations for his decision to create a Reciprocity Policy and shut down public access to Graph API were two-fold: (1) restrain competition in a wide range of software markets to make room for new products from Facebook and its close partners; and (2) shut down all mechanisms for apps to grow organically in order to force apps to prop up Facebook’s new mobile advertising business or else Facebook would shut them down. The first motivation helped ensure that no new competitive threat could ever become as big as Facebook; the second motivation ensured that Facebook could make the transition from desktop to mobile without experiencing a significant drop in revenues in order to turn around the underperforming business.” 5AC ¶ 209 (73:5-13); 4AC ¶ 203 (63:18-26).</p> <p>“At least by 2012, Zuckerberg personally oversaw a practice to weaponize Platform APIs, including a wide range of user and friend data, by inducing companies to rely on this data and then threatening to remove access unless these companies made exorbitant purchases in Facebook’s nascent mobile advertising product, known internally as ‘Neko’ ads and publicly as</p>
---	--


“Mobile App Install” ads. Zuckerberg blacklisted any companies that refused to buy these Neko ads in exchange for continued access to data that Facebook claimed for years was publicly available at no charge. This blacklisting practice also applied to companies that Zuckerberg in his sole discretion considered competitive with current or future Facebook products, even products Facebook had not yet built, and notwithstanding that most of these developers operated entirely within Facebook’s rules.

Zuckerberg’s decision to weaponize a platform economy that Facebook represented for years as open, fair and neutral stemmed from a simple fact that by 2012 had devastating consequences for Facebook: people began accessing the Internet primarily from their phones, but Facebook had built its advertising business for desktop computers, which caused Facebook’s revenues and stock price to plummet. Facebook lost over \$200 million in the second and third quarters of 2012 because it had no mobile advertising business. By mid-2012, Facebook’s most senior executives explored ways to leverage the fact that hundreds of thousands of companies relied on Facebook Platform in order to reboot its business for smartphones, presenting various options for restricting public Platform APIs to its Board of Directors in August 2012, including: [redacted]. In November 2012, after many months of discussion, Zuckerberg made his final decision to implement a version of the reciprocity policy called ‘full reciprocity,’ instead of implementing a public pricing program like Twitter or a revenue share model like the neutral platforms operated by Apple and Google - the top Platform executive, Vernal, referred to this decision as [redacted] outside Zuckerberg’s presence. Zuckerberg’s full reciprocity policy caused Facebook’s privacy and policy apparatus to disintegrate in favor of an arbitrary enforcement environment in which Facebook offered user data, and in particular friend data, to certain developers that were willing to reciprocate with Facebook, typically by agreeing to purchase no less than \$250,000 per year in unrelated Neko ads, while other developers that Facebook considered competitive were blacklisted from


	<p>accessing this data even though they never broke any rules or violated anyone's privacy.</p> <p>[redacted]. Facebook publicly announced an intentionally vague reciprocity policy in January 2013 that refused to define a 'competitive' service or 'core functionality' in order to mislead companies into thinking that only online social networks (e.g. MySpace, LinkedIn) would be considered competitive; but Facebook's internal definition of a competitive service included virtually every kind of consumer application, including those Facebook explicitly induced in its reciprocity announcement to continue using APIs it had already decided to shut down. This enabled Facebook to use its policies as an excuse to eliminate any developer for any reason whatsoever....</p> <p>The 'full reciprocity' policy was unworkable as an actual policy but was extremely effective as a 'get out of jail free' card by giving Facebook: (1) an excuse to threaten to or actually shut down certain developers unless they purchased mobile ads or provided other consideration Facebook deemed valuable in its sole discretion; (2) the ability to blame developers for privacy violations related to data Facebook chose to funnel to developers without any privacy controls; and (3) cover to continue to induce developers to rely on the very APIs Zuckerberg had decided to privatize in 2012 in order to gain more leverage. Under cover of the full reciprocity policy, the Growth team (Olivan) illegally accessed non-public information about competitive applications in order to monitor their popularity and then directed the Platform team (Vernal) to shut down an application once it became widely used. By early 2013, armed with an official reciprocity policy vague enough for Zuckerberg to consider any company a criminal, the initial pay-to-play tests began paying off as Neko ads grew faster than anyone's wildest expectations." Opposition to Individual Defendants' Anti-SLAPP Motion, filed May 17, 2018, at 4-8.</p>
	<p>"Zuckerberg and the Conspiring Facebook executives requested that Facebook employees actively conceal the decision to restrict data access to competitors from internal employees,</p>

	<p>Developers, and the public. Upon information and belief, the Conspiring Facebook Executives made various layers of management aware of this decision on a need-to-know basis periodically from late 2012 until late 2013 and, at all times, required such employees to actively conceal and/or make only partial disclosures of these material facts.” 5AC ¶ 112 (49:20-26); 4AC ¶ 106 (40:21-27).</p> <p>“Zuckerberg tasked Sukhar and Vernal, among others, with propagating this fraudulent narrative internally to Facebook employees and externally to Developers and the public. Upon information and belief, Sukhar, Vernal, and the other Conspiring Facebook Executives actively participated and conspired in the propagation of this fraudulent narrative.” 5AC ¶ 127 (56:6-10); 4AC ¶ 121 (47:3-7).</p> <p>“Beginning in 2013 and coalescing around February 2014, Zuckerberg concocted and disseminated a completely fabricated narrative to mask the deceptive and anti-competitive schemes that Zuckerberg and the other Facebook executives had decided upon and began implementing in 2012. This fabricated narrative centered on the fact that the data being shut off to tens of thousands of smaller software companies was rarely used and/or violated user trust and control over their data.... These fabricated reasons for shutting off data critical to the functioning of tens of thousands of applications played no role in the actual decisions made by Zuckerberg and ratified and implemented by other Facebook executives.” 5AC ¶ 10 (6:11-16); 4AC ¶ 10 (6:6-14).</p>
	<p>“From late 2013 through early 2014, Zuckerberg worked with the Conspiring Facebook Executives and other companies to construct a fraudulent narrative around ‘user trust’ designed to mask the true reasons he decided to close access to Facebook’s allegedly Open Graph. Upon information and belief, Zuckerberg personally decided to announce the closing of Graph API at F8 on April 30, 2014 and personally drafted his speech that actively, maliciously and fraudulently suppressed material information and revealed only partial information.” 5AC ¶ 124 (55:16-22); 4AC ¶ 118 (46:14-20).</p>


	<p>“Facebook concealed the anti-competitive Graph API Data restrictions behind a revamp of its Login product in order to cloak these changes under a narrative about user control and privacy.” 5AC ¶ 224 (80:10-12); 4AC ¶ 218 (70:9-11).</p> <p>“Zuckerberg, Vernal and Facebook Director of Engineering Doug Purdy, aggressively sought to make Defendant Sukhar the front man externally for this bait and switch scheme, which Sukhar resisted until late 2013 because he knew the conduct was wrong and malicious. However, in late 2013, Sukhar conceded and from that time on actively ratified, acquiesced in and advanced key components necessary to the implementation of the fraudulent and anti-competitive scheme in 2014 and 2015.” 5AC ¶ 85 (38:4-9).</p>
	<p>“Zuckerberg’s statement and Facebook’s subsequent announcement that certain endpoints would be removed because they were rarely used was false, and the Conspiring Facebook Executives knew them to be false at the time they made them. Upon information and belief, certain of the endpoints in question were among the most used data in Graph API.” 5AC ¶ 137 (59:9-12); 4AC ¶ 131 (50:3-6).</p> <p>“Graph API explicitly removed endpoints that were of high value to Developers, like the ability to access photos, which for years Facebook had touted as one of its most valuable and highly trafficked features in order to entice developers to build applications. Facebook’s only justification for removing access to photos at that time was that this endpoint was ‘rarely used’, which contravenes every public statement Facebook had previously stated for over seven years in which Photos were consistently touted as its #1 application and driver of user engagement.” 5AC ¶ 139 (60:1-7); 4AC ¶ 133 (50:21-27).</p> <p>“Instead, Facebook noted in its public announcement only that some ‘rarely used’ APIs would be shut down. This statement was false, and Defendants knew it to be false at the time they made it. In fact, the endpoints shut down on April 30, 2015 (the very same ones Zuckerberg secretly restricted in October and November</p>

	<p>2012) were the most widely used APIs in Facebook Platform.” SC ¶ 163 (64:3-7).</p> <p>“Once Zuckerberg decided to remove the Graph API Data to competitors, Zuckerberg personally maintained an ever-growing list of competitors that only he could authorize blacklisting from the Graph API Data. Upon information and belief, once a Developer was blacklisted from the Graph API Data, any applications the Developer built could no longer use any of the blacklisted data that Facebook purportedly provided publicly on fair and neutral terms to all Developers. Upon information and belief, blacklisted data often included the Graph API data, including the full friends list, friends permissions and newsfeed APIs – data types that were among the most popular on Facebook Platform and upon which 643’s business and many other businesses depended.” 5AC ¶ 211 (74:7-15); 4AC ¶ 205 (64:19-27).</p> <p>“The evidence submitted by Plaintiff supporting these claims consists of a large volume of internal discussions among Facebook employees regarding Defendants’ motivations for, and implementation of, various decisions related to access to Facebook’s software APIs, primarily from 2012 to 2015, as well as reliance by Plaintiff on false representations concerning such access and damages suffered by Plaintiff when the promised access was eliminated, including interference in its contractual and prospective relations with customers.” Proposed Order Denying Individual Defendants’ Special Motion to Strike, filed July 9, 2018, at 11.</p>
	<p>“Facebook’s public disclosure that it made these changes out of respect for user privacy is undermined by numerous Facebook projects that deliberately, willfully, intentionally, recklessly and negligently violated privacy by only making partial disclosures to Developers regarding how Facebook collected, stored, and transmitted user data. Upon information and belief, beginning at least by 2012, Olivan directed a range of projects under the supervision and direction of Zuckerberg, Cox and Lessin that deliberately, intentionally, maliciously, recklessly and negligently violated user privacy in order to effectuate Facebook’s anti-competitive scheme of</p>



	<p>baiting companies to rely on Facebook Platform.” 5AC ¶ 226 (80:25-81:6); 4AC ¶ 220 (70:25-71:5).</p> <p>“The FTC Order provided, among other things, that Facebook and its representatives “shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information. The FTC Order defined “covered information” to include an individual consumer’s photos, among other things. The FTC Order also provided that Facebook and its representatives “shall not misrepresent in any manner, expressly or by implication...the extent to which [Facebook] makes or has made covered information accessible to third parties.” 5AC ¶¶ 82-84 (36:15-25); 4AC ¶¶ 76-78 (29:3-10).</p> <p>“The conduct of Zuckerberg and the Conspiring Facebook Executives was wrongful on a number of independent grounds, including violation of California’s Unfair Competition law (including violation of the FTC Order), and the common law causes of action for intentional misrepresentation, negligent misrepresentation, and concealment.” 5AC ¶ 297 (99:10-13); 4AC ¶ 281 (86:1-4).</p> <p>List of almost a dozen privacy-violating projects. 5AC ¶¶ 227-233; 4AC ¶¶ 220-227.</p>
	<p>“Facebook directed a project to collect certain data from consumers who had downloaded the Onavo app, a virtual private network app downloaded by approximately 30 million people, which Facebook purchased in October 2013. Upon information and belief, before the WSJ article, Facebook failed to disclose that it used Onavo data to measure what people do on their phones beyond Facebook’s own suite of apps, including detailed information on things such as which apps people generally are using, how frequently, for how long, and whether more women than men use an app in a specific country.... Facebook failed to disclose that it used this data for competitive intelligence of numerous apps.... Facebook’s decision to purchase a large competitive application (WhatsApp) was heavily influenced by Facebook’s ability to obtain this non-public information from Onavo... Had Facebook fully disclosed this deceptive practice publicly to users and Developers when it made</p>

	<p>public disclosures regarding its purchase of Onavo and its update to Onavo's Terms of Service, then 643 would not have invested in or continued to invest in building its business." 5AC ¶ 227 (81:21-82:11); 4AC ¶ 221 (71:21-72:9).</p> <p>"Olivan accomplished this by monitoring apps installed on the phones of 30 million people who had installed Onavo, a virtual private network app that Facebook bought in 2013; Olivan was able to track highly sensitive information about at least 82,000 software applications as a result of violating the privacy of these 30 million people." Opposition to Individual Defendants' Anti-SLAPP Motion, filed May 17, 2018, at 8, fn. 15.</p>
	<p>"At least by 2012 or 2013, Facebook collected various content and metadata regarding communications on Android Phones without fully disclosing this to Facebook's users." 5AC ¶ 228 (82:12-14); 4AC ¶ 222 (72:10-12).</p> <p>"At least by 2013 and continuing at least through 2015, Facebook continued to explore and implement ways to track users' location, to track and read their texts, to access and record their microphones on their phones, to track and monitor their usage of competitive apps on their phones, and to track and monitor their calls. For example, upon information and belief, Facebook expanded its program to access and monitor the microphone on Android phones in 2015 without securing the explicit consent of all users and while only providing partial disclosures as to what information was being obtained and for what purposes it was being used." 5AC ¶ 233 (84:10-17); 4AC ¶ 227 (73:23-74:2).</p>
	<p>"Facebook deliberately ignored the privacy settings of a Facebook user's friend list in order to improve a certain prominent feature in the Facebook app and website. Upon information and belief, Facebook made partial public disclosures of this practice while withholding material facts that, if disclosed, would have materially qualified Facebook's public statement." 5AC ¶ 229 (83:1-6); 4AC ¶ 223 (72:24-28) (refers directly to an article discussing the People You May Know feature: <a href="https://gizmodo.com/facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163">https://gizmodo.com/facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163</a>)</p>

	<p>“In 2013 and 2014 Facebook deliberately implemented code to have a user’s privacy setting lapse after a period of time, requiring the user to go through additional effort in order to have the user’s privacy settings respected. Facebook made partial disclosures around this time regarding privacy settings, but did not fully disclose that it had caused certain settings to lapse after a period of time. Upon information and belief, at all times, the employees involved in this project were acting under the direction and approval of Zuckerberg, Cox, Lessin and Olivan.” 5AC ¶ 231 (83:18-24); 4AC ¶ 225 (73:9-15); <i>see also</i> 5AC ¶ 226; 4AC ¶ 220 (Zuckerberg directly overseeing all of these privacy-violating requests)</p> <p>“By way of example, if User A uploaded a photo to Facebook and set the photo to ‘only me,’ only User A would be able to see the photo on Facebook.com or in the Facebook mobile app. However, because the Apps Others Use setting was hidden, not explained to users, and had the default set to ‘on’ (issues the FTC had identified in its Complaint and Order), this meant that when User B used a Developer’s app, User B would be able to see User’s A photo that was set to “only me” if User B was friends with User A. This is because Facebook did not pass the privacy settings of a data object in the most widely used Graph API endpoints, and because Facebook had ‘auto-consented’ User A to share this data in Apps Others Use without revealing this fact to User A. User B sees the photo and tells User A, and User A complains that the Developer is violating their privacy when in fact it was Facebook. The Developer could not have even known that User B was not supposed to see User A’s photo since Facebook falsely represented it handled such settings prior to sending the photo to the Developer.” SC ¶ 113 (46:5-16)</p>
---	---